IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Peter Secor, et al.	)	
	)	
Serial No.: 10/756,843	)	Group Art Unit: 2152
	)	
Filed: January 13, 2004	)	Examiner: Brian P. Whipple
	)	
For: METHOD AND SYSTEM FOR	)	
NETWORK EVENT IMPACT	)	
ANALYSIS AND CORRELATION	)	
WITH NETWORK	)	
ADMINISTRATORS,	)	
MANAGEMENT POLICIES AND	)	
PROCEDURES	)	

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

In support of the Notice of Appeal filed on August 22, 2008, and pursuant to 37 C.F.R. § 41.37, Appellants present this appeal brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 4-23 in the Final Office Action dated June 4, 2008. The appealed claims are set forth in the attached Claims Appendix.

1.   Real Party in Interest

        This application was assigned to Micromuse Inc., which was acquired by

International Business Machines Corporation, the real party in interest.

2.   Related Appeals and Interferences

        There are no other appeals or interferences which would directly affect, be

directly affected by, or have a bearing on the instant appeal.

3.   Status of Claims

        Claims 1-3 have been cancelled. Claims 15-23 stand finally rejected under 35

U.S.C. §101. Claims 4-23 stand finally rejected under 35 U.S.C. §102(e). The final

rejections of claims 4-23 is being appealed.

4.   Status of Amendments

        All amendments submitted by the Appellant have been entered.

5.   Summary of Claimed Subject Matter

        Claim 4 recites a method for handling network events generated in a network in

an enterprise. (see, for example, page 3, line 15 - page 4, line 1). The method comprises

detecting at least one of a plurality of network events. (see, for example, page 12, lines

5-9). The method comprises executing an action tree in response to the network event,

the action tree including instructions based on relationships between enterprise-related

data objects. (see, for example, page 12, lines 10-16, page 12, line 22 - page 13, line 7).

The relationships defined by at least one data impact analysis data structure are populated

with data accessed from a plurality of data sources throughout the network. (see, for

example, page 4, lines 17-22, page 7, line 2 - page 8, line 2).

Claim 15 recites an apparatus for handling network events generated in a network in an enterprise. (see, for example, Fig. 1, page 3, line 15 - page 4, line 1). The apparatus comprises an event broker operative to detect at least one of a plurality of network events. (see, for example, Fig. 1 element 114, page 12, lines 5 - 9). The apparatus comprises an impact server operative to execute an action tree in response to the network event, the action tree including instructions based on relationships between enterprise-related data objects. (see, for example, Fig 1 element 100, page 12, lines 10-16, page 12, line 22 - page 13, line 7) The relationships defined by at least one impact analysis data structure are populated with data accessed from a plurality of data sources throughout the network. (see, for example, page 4, lines 17-22, page 7, line 2 - page 8, line 2).

6.   Grounds of Rejection to be Reviewed on Appeal

I.   The rejection of claim 15 under 35 U.S.C. §101 is improper because the claim properly recites statutory subject matter.

II.   The rejection of claims 4 and 15 under 35 U.S.C. §102(e) is improper because U.S. Patent No. 6,470,384 (O'Brien) fails to identically disclose all of the claimed limitations.

7.   Argument

I.   The rejection of claim 15 under 35 U.S.C. §101 is improper because the claim properly recites statutory subject matter..

The rejection of claim 15 under 35 U.S.C. §101 is improper because the claim properly recites statutory subject matter.

Claim 15 was finally rejected under 35 U.S.C. §101 as being "directed to non-statutory subject matter." Appellants respectfully disagree and submit the Examiner's reasoning and legal support is flawed.

The Examiner states that "the specification leads to the conclusion that the apparatus of the claimed invention may be implemented in software" and that "software fails to fall into one of the four statutory classes of invention: process, machine, manufacture, or composition of matter." First off, the Examiner overlooks the **exact** language of claim 15 which recites "An apparatus .. . comprising ... an event broker ... and an impact server." The event broker 114 of Fig. 1 is described in the specification as a "module that provides for real time event processing." The impact server 100 of Fig. 1 is described as being within the "logic layer."

Pursuant to 35 U.S.C. §112, ¶1, the specification "shall contain a written description of the invention … as to enable any person skilled in the art to which it pertains." It is recognized by one skilled in the art, as per the standard under 35 U.S.C. §112, ¶1, that a module is implemented in a processing device and the logic layer is also a physical processing device physically performing processing operations.

In the final Office Action dated June 4, 2008 on pages 2-3, the Examiner states a failure "to see how a module and a server in the logical layer are statutory embodiments and not software as previously discussed. A software module and a logical server are not statutory embodiments as defined under 35 U.S.C. 101." Appellants respectfully disagree because the Examiner overtly includes descriptive terminology outside of **the exact language of the claims**.

The Examiner refers to "a software module" and "a logical server," whereas claim 15 recites "an event broker" and "an impact server."

For example, the specification describes the impact server 100 including two processors 116, 118, as well as a two databases 102 and 120 (see, for example, Fig. 1).

The Examiner's interpretation and assertion that the "impact server" is a logical server and in-fact merely software is in direct contradiction to the exact disclosure of the specification, as well as in direct contradiction to the Examination standard under 35 U.S.C. §112, ¶1.

The specification also refers to the event broker as a "module that provides for real time event processing," where again under the 35 U.S.C. §112, ¶1 standard, it is understood that software does not and cannot exist in vacuum. Rather, the description of providing for real-time event processing requires a physical processing component for the performance of this operation, again fully consistent with the Examination standard under 35 U.S.C. §112, ¶1.

Hence, Appellants submit this rejection is improper because claim 15, and hence claims 16-23 as well, fall within a statutory subject consistent with 35 U.S.C. §101.

II.   The rejection of claims 4 and 15 under 35 U.S.C. §102(e) is improper because U.S. Patent No. 6,470,384 (O'Brien) fails to identically disclose all of the claimed limitations.

Claims 4 and 15 stand finally rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,470,384 (O'Brien). Appellants respectfully disagree and submit this rejection is improper because O'Brien fails to identically disclose all of the claimed limitations.

O'Brien describes a multi-computer network that includes action sets for the performance of various activities, typically security activities, in response to detected network events under the Simple Network Management Protocol (SNMP). Agents 6 generate network events 7 and a manager 25 (also known as the arbiter 8) maps the

network events to actions 32. These actions are then performed by the actors 9. (col. 4, lines 35-39). Network events are generally defined as any type of "state or condition" that can "be monitored and reported to the arbiter 8." (col. 4, lines 39-41). In response to the event notification, the manager "determines the set of actions to which the network event 7 is associated using a stored set of event mappings." (col. 4, line 65 - col. 5, line 2). O'Brien further describes that network includes active security features by scanning agents scanning the network and if security issues are detected, certograms are provided to the manager 25, where certograms are "specialized messages."

Claims 4 and 15 recites the execution of the action tree "in response to the network event, the action tree including instructions based on relationships between enterprise-related data objects, the relationships defined by at least one data impact analysis data structure populated with data accessed from a plurality of data sources throughout the network."

Among other shortcomings, Appellants submit that O'Brien fails to identically disclose the claimed "action tree" where the action tree includes "instructions based on relationships" as claimed including the "relationships defined by at least one data impact analysis data structure populated with data accessed from a plurality of data sources through the network."

O'Brien describes manager 25 accessing the stored set of event mappings (col. 4, line 66 - col. 5, line 5) and the active security agent 23 scanning the network and notifying the manager 25 of any vulnerabilities (col. 5, lines 19-24). These passages, as well as O'Brien in general, do not provide the claimed "relationships" as O'Brien does

not generate instructions that are based on relationships defined by at least one data impact analysis data structure populated with data access from a plurality of data sources.

Among other deficiencies, O'Brien does not include "data impact analysis data structure" where this "data structure" is "populated with data accessed from a plurality of data sources." Rather, at best, the manager 25 of O'Brien can, in response to the certograms 30, generate an action set to be taken by, in this example, a firewall 17. (col. 6, lines 47-50).

On page 4 of the final Office Action dated June 4, 2008, the Examiner asserts that under O'Brien, "mapping network events to appropriate actions is defining relations." Appellants respectfully disagree and submit this overlooks the exact claim language as recited, which includes that "the relationships <u>defined by at least one data impact analysis data structure</u>," the relationships are "between enterprise-related data objects." The Examiner-cited passages provide for the arbiter 8 to map events 7 to actions 32, where the events are "any type of state or condition which could be monitored and reported" and actions are functions the system can perform. In other words, the O'Brien system merely maps a system function to a device that can perform that function. This is inconsistent with "relationships between enterprise-related data objects" and does not disclose the "data impact analysis data structure."

The shortcomings of O'Brien are further emphasized where in the Final Office Action, page 4, the Examiner further asserts that O'Brien discloses the data impact analysis data structure is populated with data accessed from a plurality of data sources throughout the network. The Examiner cites to col. 5, lines 19-24, which describes the generation of certograms by scanning the system. As noted above, certograms are

"specialized messages," where these message relate to any detected vulnerabilities. "The active security scanner agent 23 proactively analyzes the security and integrity of the network and reports any vulnerabilities ... using specialized messages known as certograms 30." (col. 5, lines 19-24). These certograms report system vulnerabilities, which is wholly inconsistent with populating a data structure with data accessed from a plurality of data sources. There is no disclosure within O'Brien and it is inconsistent with O'Brien and the security operations to use these certograms to populate a data structure that defines relationships between enterprise-related objections. Rather, the certograms are notifications that warrant the manager to perform a particular activity.

The Examiner further cites to col. 7, lines 20-24 and lines 46-54. These passages describe SNMP traps, which includes an event mapping being referenced by object identifiers (OID). The event mapping even includes referencing additional actions. Appellants again assert this overlooks the exact language of claims 4 and 15, which recite "the relationships defined by at least one data impact analysis data structure populated with data accessed from a plurality of data sources throughout the network." (emphasis added). The event mappings do not identically disclose the population of the data structure with data accessed from a plurality of data sources, rather the event mappings of O'Brien include directions for the performance of a security operation and who may perform the operation. Event mappings are absolutely silent regarding data being accessed from a plurality of data sources and in fact O'Brien does not "populate" any data structure, rather uses a define roadmap for the performance of an "action set 39" in response to "a network event 7," where the action set includes "at least one action 32."

Accordingly, Appellants respectfully submit that O'Brien does not identically disclose the claimed limitations recited in claims 4 and 15 (as well as dependent claims 5-14 and 16-23), and therefore the present rejection is improper.
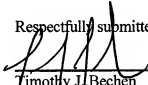
Conclusions

For the reasons set forth above, Appellant respectfully requests that the Board reverse the final rejections of the claims by the Examiner under 35 U.S.C. § 101 and §102(e) and indicate that claims 4-23 are allowable.

Dated: October 22, 2008

Respectfully submitted,

_____
Timothy J. Bechen
Reg. No. 48,126
DREIER LLP
499 Park Ave.
New York, New York 10022
Tel : (212) 328-6100
Fax: (212) 328-6101

Customer No. 61834

THIS CORRESPONDENCE IS BEING SUBMITTED
ELECTRONICALLY THROUGH THE PATENT AND
TRADEMARK OFFICE EFS FILING SYSTEM ON
October 22, 2008.

Claims Appendix

1. - 3. (Cancelled)

4. (Previously Presented) A method for handling network events generated in a network in an enterprise, the method comprising:

detecting at least one of a plurality of network events; and

executing an action tree in response to the network event, the action tree including instructions based on relationships between enterprise-related data objects, the relationships defined by at least one data impact analysis data structure populated with data accessed from a plurality of data sources throughout the network.

5. (Previously Presented) The method of claim 4 further comprising:

identifying a workstation affected by the detected network event;

determining at least one administrator and at least one business unit affected by the network event; and

contacting the at least administrator regarding the detected network event.

6. (Previously Presented) The method of claim 5, wherein the step of determining at least one administrator and at least one business unit includes the determination being made by traversing the impact data analysis data structure.

7. (Previously Presented) The method of claim 4, wherein the execution of the action tree is performed by a policy engine.

8. (Previously Presented) The method of claim 4, wherein the enterprise-related data objects include organization nodes that define the organization structure of the enterprise.

9. (Previously Presented) The method of claim 8, wherein the organizational structures include at least one of: a host, a communication device, a user and a document.

10. (Previously Presented) The method of claim 8 further comprising:

accessing the enterprise-related data objects through a networked database.

11. (Previously Presented) The method of claim 4 further comprising:

hibernating the action tree, including saving a current state of the action tree to a

state database.

12. (Previously Presented) The method of claim 11, wherein the state database is

within an impact server.

13. (Previously Presented) The method of claim 11 further comprising:

awakening the action tree from a hibernated state in response to a wakeup call

message.

14. (Previously Presented) The method of claim 13, wherein the wakeup call

message is an electronic mail message.

15. (Previously Presented) An apparatus for handling network events generated

in a network in an enterprise, the apparatus comprising:

an event broker operative to detect at least one of a plurality of network events;

and

an impact server operative to execute an action tree in response to the network

event, the action tree including instructions based on relationships between enterprise-

related data objects, the relationships defined by at least one impact analysis data

structure populated with data accessed from a plurality of data sources throughout the

network.

16. (Previously Presented) The apparatus of claim 15, wherein the impact server

is further operative to identify a workstation affected by the detected network event,

determine at least one administrator and at least one business unit affected by the network event and contact the at least administrator regarding the detected network event.

17. (Previously Presented) The apparatus of claim 15 further comprising:

a policy engine disposed within the impact server, wherein the execution of the action tree is performed by the policy engine.

18. (Previously Presented) The apparatus of claim 17, wherein the enterprise-related data objects include organization nodes that define the organization structure of the enterprise.

19. (Previously Presented) The apparatus of claim 18, wherein the organizational structures include at least one of: a host, a communication device, a user and a document.

20. (Previously Presented) The apparatus of claim 15 further comprising:

a networked database having the enterprise-related data objects stored therein, such that accessing the enterprise-related data objects through a networked database.

21. (Previously Presented) The apparatus of claim 15 further comprising:

a state database; and

the impact server is further operative to hibernate the action tree, including saving a current state of the action tree to the state database.

22. (Previously Presented) The apparatus of claim 21, wherein the impact server is further operative to awaken the action tree from a hibernated state in response to a wakeup call message.

23. (Previously Presented) The apparatus of claim 22, wherein the wakeup call message is an electronic mail message.

Evidence Appendix

No evidence has been submitted or relied upon in the instant appeal.

Related Proceedings Appendix

There are no related proceedings which are related to or would have a bearing on the instant appeal.